TMA Privacy Office Information Paper

ACCESS CONTROLS

HIPAA Security ◆ November 2003

STANDARD REQUIREMENT

Covered entities must implement information system access controls as part of their technical safeguards. The access controls at issue here are defined as "technical policies and procedures for electronic information systems that maintain protected health information to allow access only to those persons or software programs that have been granted access rights as specified in" the information access management standard under administrative safeguards. Those administrative policies and procedures identify and determine the access rights and privileges of authorized users. A covered entity's IT systems must enforce those administrative policies.

IMPLEMENTATION SPECIFICATIONS

The access control standard has four implementation specifications. The first two are required and the last two addressable:

- unique user identification;
- emergency access procedure;
- automatic logoff; and
- encryption and decryption.

The first implementation specification, unique user identification, requires assigning "a unique name and/or number for identifying and tracking user identity." The Rule permits "any appropriate access control" mechanism in conjunction with unique user identification. (Final Rule, p.8355) Each covered entity must assign a name and/or number to each user specific to that and only that user. System processes will use this name and/or number to identify the user and to associate the user with tracked actions taken by or on behalf of that user. Without unique user identifiers audit logs are not useful in assessing inappropriate access to electronic protected health information (EPHI) by individual users.

The second implementation specification, emergency access procedure, requires establishing — and implementing, as necessary — procedures for "obtaining necessary electronic protected health information during an emergency." The Final Rule commentary notes that "access controls will still be necessary under emergency conditions, but they may be very different from those used under normal operational circumstances." (Final Rule, p.8355) Each covered entity must develop technical procedures, and document instructions, for obtaining EPHI when the normal methods for obtaining access fail because of a crisis situation. Two situations may potentially deny access to patient information stored in automated information systems, including system failure and the unavailability of authorized users. This mandatory implementation specification requires covered entities to develop procedures to grant temporary access to otherwise unauthorized providers when a patient's authorized providers may not be available (such as, during admission to a hospital Emergency Department).

Covered entities should specify procedures for gaining access to information during a system emergency or failure as part of the security management plan.

The third implementation specification, automatic logoff, covers procedures that "terminate an electronic session after a predetermined time of inactivity." Because this requirement is "addressable", compliance depends on the outcome of a covered entity's risk assessment. Covered entities should evaluate the need for, and interval of inactivity that triggers an automatic logoff. A covered entity should determine the need for and the strength of the mechanism of automatic logoff through its risk assessment. As with all addressable implementation specifications an equivalent measure that achieves inactivity lockout is permissible when an automatic logoff is not reasonable or appropriate. (Final Rule, p.129-130) A covered entity should describe and justify its approach to these controls in its risk management plan.

The last implementation specification, encryption and decryption, focuses on the use of "mechanism[s] to encrypt and decrypt electronic protected health information." Because this requirement is "addressable", compliance depends on the outcome of a covered entity's risk assessment. This is the first of two times that encryption appears in the final rule and it is important to understand why. The rule as originally proposed uses the same general definition each time encryption appears as an addressable implementation specification thus obscuring the differences between the requirements. The differences in meaning become clear only when taken in context with their associated categories and requirements. The final rule changes the wording to put the requirements in context and clarify the rule's intent. In this specific provision "encryption" is associated with the "Access Control" standard to function as a means of controlling access to protected health information during storage or transmission. Examples of access controlled by this method include encrypting the database or files of sensitive information and encrypting information en route between a client and server. The risk assessment of each covered entity should determine if encryption of files in storage or transmission is an appropriate method to control access to PHI on their systems based on the nature of the risk, the cost, and their business environment. The covered entity's risk management plan should describe and justify its approach to this issue.

See also:
45 CFR 164.308(a)(4), 310(a)(1), 312(a)(1)

Federal and DoD regulations that support this standard
DoD 8510.1-M
Controlled Access Protection Profile
DoDD 8500.1
DoDI 8500.2